

Ärende nr: Svk 2026/3987

Datum: September 2026

Öppen antagonistisk hotbild mot svensk elförsörjning



Svenska kraftnät

Svenska kraftnät är en myndighet som utifrån ett samhällsbyggnadsperspektiv skapar förutsättningar för en samhällsekonomiskt effektiv, internationellt konkurrenskraftig, hållbar och trygg elförsörjning i Sverige.

Myndigheten har i uppdrag att förvalta, driva och utveckla transmissionsnätet så att samhällets behov av el möts i alla lägen, samt för utvecklingen av elmarknadens funktion.

Svenska kraftnät ansvarar dessutom för elberedskap, tillsyn samt för vägledning kring dammsäkerhet.

Mer information finns på svk.se

Version **1.0**
Org. nr 202 100-4284

Svenska kraftnät
Box 1200
172 24 Sundbyberg
Sturegatan 1

Tel: 010-475 80 00
Fax: 010-475 89 50
www.svk.se

Innehåll

Sammanfattning	5
1 Inledning.....	7
1.1 Syfte.....	7
1.2 Källor	8
1.3 Målgrupp.....	8
2 Hoten mot Sverige	8
2.1 Omvärldsläget	8
2.1.1 Hybridhot.....	9
3 Hoten mot elförsörjningen	10
3.1 Hotbild mot elförsörjningen.....	10
3.2 Typer av antagonistiska hot mot elförsörjningen	10
3.3 Hotaktörer	11
3.3.1 Ryssland.....	12
3.3.2 Kina	12
3.3.3 Iran	13
3.3.4 Organiserad brottslighet	14
3.3.5 Våldsbejakande extremism.....	15
3.4 Mål inom elförsörjningen	17
3.4.1 Konfidentialitet	18
3.4.2 Riktighet.....	18
3.4.3 Tillgänglighet.....	19
3.4.4 Andra typer av mål	19
3.5 Hotbildens föränderlighet och vad det medför	20
4 Antagonistiska hot.....	21
4.1 Cyberhot.....	21
4.1.1 AI:s betydelse för cyberhotbilden	22
4.1.2 Aktuella händelser	23
4.2 Fysisk skadegörelse och sabotage	24
4.2.1 Aktuella händelser	25

4.3	Informationsinsamling.....	26
4.3.1	Aktuella händelser	28
4.4	Strategiska uppköp och investeringar.....	29
4.4.1	Aktuella händelser	30
4.5	Utkontraktering och osäkra leveranskedjor.....	32
4.5.1	Aktuella händelser	32
4.6	Informationspåverkan.....	33
4.6.1	Aktuella händelser	35
	Referenser i urval.....	37
	Samlingssidor för svenska underrättelsemyndigheters årsöversikter	37
	Svenska myndigheter i övrigt	37
	Utländska myndigheter.....	38

Sammanfattning

Svenska kraftnät bedömer att de hot som svensk elförsörjning möter i grunden är av samma art idag som för några år sedan. Samtidigt är vissa av dem, som cyberhotet, i ständig förändring och det försämrade säkerhetsläget har gjort att vissa hot är än mer aktuella än tidigare.

Den samlade bedömningen från underrättelsemyndigheterna är att hotbilden är fortsatt allvarlig och komplex. Enligt Säkerhetspolisen bedriver främmande makt systematiskt säkerhetshotande verksamhet mot Sverige inom ett stort antal områden och beskriver Ryssland, Kina och Iran som de främsta hotaktörerna. Ryssland anses utgöra det största och mest allvarliga hotet med ett mer riskbenäget och offensivt agerande än tidigare.

Svenska kraftnät delar de svenska underrättelsemyndigheternas bedömning – de största hoten mot svensk elförsörjning kommer från Ryssland, Kina och Iran. Underrättelsemyndigheterna lyfter särskilt det civila försvaret som ett utpekad mål för Rysslands informationsinhämtning, och då specifikt svensk energiförsörjning. Även för cyberangrepp och sabotageverksamhet bedöms energiförsörjningen vara en måltavla.

De främsta antagonistiska hoten som Svenska kraftnät ser gentemot svensk elförsörjning är, utan inbördes rangordning:

- Cyberhot
- Fysisk skadegörelse och sabotage
- Informationsinsamling
- Strategiska uppköp och investeringar
- Utkontraktering och osäkra leverantörskedjor
- Informationspåverkan

Mål inom elförsörjningen för en antagonistisk aktör kan vara fysisk infrastruktur, infrastruktur och system för IT och OT, information och personal. En angripare kan också välja att närma sig dessa mål genom leverantörer av varor eller tjänster som verksamheten är beroende av.

Genom denna öppna antagonistiska hotbild delar Svenska kraftnät en generell hotbild för elförsörjningen som helhet. Målet är att bidra till att utveckla säkerhets- och beredskapsarbetet inom svensk elförsörjning. Varje verksamhet behöver göra en egen analys av hotbilden mot den egna verksamheten och hur den påverkas av exempelvis utvecklingen i omvärlden. En aktörs avsikt kan snabbt förändras, vilket gör att hotbilder

är en färskvara. Svenska kraftnät uppmanar därför organisationer verksamma inom elförsörjningen att löpande bevaka uttalanden från myndigheterna inom underrättelseområdet.

Verksamhetsutövare inom elförsörjningen bör också vara vaksamma på lägesbilden för sin egen verksamhet. Fokus behöver ligga på vad som utgör vardag, den så kallade normalbilden, och vad som avviker från denna. Information och anmälningar till Säkerhetspolisen är avgörande för att Säkerhetspolisen ska kunna upprätthålla och förbättra sin lägesbild gällande hoten mot Sverige, inklusive mot elförsörjningen.

1 Inledning

I Svenska kraftnäts öppna antagonistiska hotbild redogörs för hotbilden mot svensk elförsörjning i fredstid. Svenska kraftnät har i framtagandet sammanställt öppna källor i syfte att dokumentera och analysera de hot som anses vara aktuella mot elförsörjningen. De öppna källorna innefattar främst publikationer från Säkerhetspolisen, Försvarets radioanstalt (FRA), Militära underrättelse- och säkerhetstjänsten (MUST), Myndigheten för civilt försvar (MCF) och Nationellt cybersäkerhetscenter (NCSC).

Rapporten är en uppdatering av den antagonistiska hotbild som Svenska kraftnät publicerade 2024.¹ Liksom i tidigare version läggs tonvikten vid den komplexa hotbilden i en allt mer osäker omvärld men flera delar har helt eller delvis uppdaterats eller skrivits om för att spegla de senare årens händelser i omvärlden och för att hänvisa till mer aktuella källor.

Främsta förändringen i den här reviderade versionen är att Svenska kraftnät lägger större tonvikt vid den föränderliga hotbilden och det ökade hybridhotet. Två antagonistiska hot som särskilt lyfts fram i denna version är cyberhotet, där framför allt artificiell intelligens (AI) driver på utvecklingen, samt informationspåverkan.

1.1 Syfte

Syftet med denna öppna antagonistiska hotbild är att dela en öppen och generell hotbild mot elförsörjningen som helhet. Målet är att därigenom bidra till att utveckla säkerhets- och beredskapsarbetet inom svensk elförsörjning. Den öppna antagonistiska hotbilden utgör även underlag till Svenska kraftnäts risk- och sårbarhetsanalys som görs enligt 7§ förordningen (2022:524) om statliga myndigheters beredskap.

Följande hotbild omfattar kända antagonistiska hot och ska inte uppfattas som heltäckande för alla hot mot elförsörjningen som kan förekomma. Denna hotbild omfattar inte heller hot under höjd beredskap och krig, även om antagonistiska ageranden, så kallade hybridhot, sker i alla samhällstillstånd.

¹ Svenska kraftnät, *Öppen antagonistisk hotbild för elförsörjningen*, SvK 2024/2196

1.2 Källor

I denna öppna hotbild beskrivs olika typer av antagonistiska hot, främst utifrån Säkerhetspolisens lägesbild 2025/2026, FRA:s årsrapport 2025, MUST årsöversikt 2025 samt MCF:s cyberincidentsrapportering 2025. Ytterligare källor är rapporter från bl.a. Totalförsvarets forskningsinstitut (FOI), Cybersäkerhetstjänsten för unionens institutioner, organ och byråer (CERT-EU) och Europeiska unionens cybersäkerhetsbyrå (ENISA).

För att dokumentet ska vara tillgängligt så baseras den enbart på öppna källor, de mest relevanta återfinns i en lista i slutet av rapporten. Svenska kraftnät uppmanar alla aktörer inom elförsörjningen att ta del av dessa öppna underlag i sin helhet.

1.3 Målgrupp

Svenska kraftnäts öppna antagonistiska hotbild riktar sig till aktörer inom elförsörjningen. Föreliggande rapport kan utgöra en grund för aktörer inom elförsörjningens arbete med sina egna hotbildsanalyser. Den är dock inte tillräcklig för att användas rakt av i exempelvis säkerhetsskyddsanalyser eller liknande utan behöver anpassas utifrån den egna verksamhetens förutsättningar. Mot bakgrund av hotbildens föränderlighet och de variationer som finns beträffande mål hos aktörer inom elförsörjningen, är det av stor vikt att varje aktör gör en individuell hotanalys.

2 Hoten mot Sverige

2.1 Omvärldsläget

Alla svenska underrättelsemyndigheter beskriver i sina senaste årsöversikter en hotbild som är fortsatt komplex och allvarlig och som präglas av geopolitisk instabilitet.² Den senaste tidens händelseutveckling i mellanöstern, där USA och Israel i februari 2026 inledde en militär operation i Iran, bidrar till en ökad osäkerhet och oförutsägbarhet vad gäller den säkerhetspolitiska utvecklingen i omvärlden, samtidigt som Rysslands anfallskrig i Ukraina alltjämt fortgår. Till detta läggs ett allt mer framträdande cyberhot där den tekniska utvecklingen, med artificiell

² De flesta är publicerade under våren 2026, se avsnitt 1.2 Källor.

intelligens (AI) som katalysator, har medfört mer lättillgängliga metoder och ökad förmåga hos aktörer att genomföra cyberangrepp.

Ryssland, Kina och Iran beskrivs fortsatt av underrättelsemyndigheterna som de främsta hotaktörerna som bedriver säkerhetshotande verksamhet mot Sverige, där Ryssland anses utgöra det största och mest allvarliga hotet med ett mer riskbenäget och offensivt agerande än tidigare. Det rör sig bland annat om underrättelseverksamhet, dolda och förnekbara påverkansaktiviteter och cyberangrepp.

Samtliga av de svenska underrättelsemyndigheterna framhåller just det ökade cyberhotet i sina respektive årsrapporter. Den vanligaste formen av främmande underrättelseverksamhet mot Sverige utgörs idag av angrepp mot IT-system med syftet att kartlägga Sveriges försvarsförmåga och sårbarheter, vilket omfattar måltavlor inom det civila försvaret och kritisk infrastruktur.³

2.1.1 Hybridhot

Hybridhot utgör en form av sammansatta hot där statliga aktörer använder en kombination av militära och icke-militära medel för att påverka, destabilisera eller skada en motståndare, utan att överskrida tröskeln för väpnat angrepp.⁴ Det kan handla om desinformation, cyberangrepp och sabotage mot kritisk infrastruktur samt politiska, ekonomiska och diplomatiska påtryckningsmedel. Tillsammans kan dessa åtgärder användas i syfte att utnyttja motståndarens svagheter för att uppnå specifika mål.⁵

För Ryssland utgör hybridkrigföring ett centralt verktyg för att nå de ryska strategiska målsättningarna och används för att påverka utvecklingen i Sveriges närområde. Även konflikten i Mellanöstern driver på ett ökat hybridhot från Iran gentemot Europa och Sverige.⁶

Att avgöra om antagonistiska attacker utförs av främmande makt som ett led i hybridkrigföring är ibland mycket svårt, vilket också ligger i sakens natur då en angripare oftast vill dölja vem som ligger bakom attacken. Enligt Säkerhetspolisen har Sverige dock ännu inte varit utsatt för

³ Försvarets radioanstalt, *Årsrapport 2025 – En farligare tid*, publicerad mars 2026.

⁴ Försvarsmakten, *MUST årsöversikt 2025*, publicerad februari 2026.

⁵ Försvarets radioanstalt (FRA), "Hybridhot", <https://fra.se/underrattelser/hybridhot.4.55af049f184e92956c42d27.html>.

⁶ Försvarsmakten, *MUST årsöversikt 2025*.

omfattande försök till hybridangrepp eller traditionella sabotage även om försök till cybersabotage från Ryssland har förekommit.

För en mer utförlig beskrivning av hotbilden mot Sverige generellt hänvisas läsaren till underrättelsemyndigheternas årsöversikter, vilka återfinns i referenslistan.

3 Hoten mot elförsörjningen

3.1 Hotbild mot elförsörjningen

Hotbilden mot svensk elförsörjningen är en del av den bredare hotbilden mot svensk samhällskritisk infrastruktur och präglas av det försämrade säkerhetspolitiska omvärldsläget.

Svenska kraftnät bedömer att hoten och hotaktörerna som föreligger mot svensk elförsörjning i huvudsak är desamma som under de senaste åren. Samtidigt medför bland annat den snabba teknikutvecklingen, ökad digitalisering, komplexare leverantörskedjor och det försämrade säkerhetsläget att nya potentiella hot tornar upp sig. Dessutom kan dessa skeenden innebära att befintliga hot kan få större konsekvenser för elförsörjningen, exempelvis cyberhotet.

Hot mot elförsörjningen kan riktas mot anläggningar, IT- eller OT-system, information, leverantörskedjor och personal. Syftet kan vara att sabotera, störa eller påverka förmågan att producera och distribuera el, alternativt att skapa osäkerhet och öka polarisering.

De hot och hotaktörer som beskrivs nedan ska inte ses som uttömmande eftersom dessa kan variera beroende på aktör inom elförsörjningen. Beskrivningen nedan utgör emellertid en översikt av de mest framträdande hoten och hotaktörerna.

3.2 Typer av antagonistiska hot mot elförsörjningen

De främsta antagonistiska hoten som Svenska kraftnät ser gentemot svensk elförsörjning är, utan inbördes ordning:

- Cyberhot – angrepp mot exempelvis IT- eller OT-system och leverantörskedjor.

- Fysisk skadegörelse och sabotage – riktat mot exempelvis anläggningar och annan kritisk infrastruktur.
- Informationsinsamling – kartläggning av anläggningar, personal och skyddsvärda uppgifter om exempelvis sårbarheter.
- Strategiska uppköp och investeringar – möjlighet till att skapa beroenden eller förutsättningar att få tillgång till skyddsvärda uppgifter och teknik.
- Utkontraktering och osäkra leverantörskedjor – risk för sårbarheter genom produkter och underleverantörer.
- Informationspåverkan – negativ påverkan på förtroende för elförsörjningen och dess förmåga, aktörer och beslutsfattare.

Dessa hot redogörs för närmare i avsnitt 4.

3.3 Hotaktörer

Svenska kraftnät delar de svenska underrättelsemyndigheternas bedömning beträffande de största statliga hotaktörerna. De största hoten mot svensk elförsörjning kommer från Ryssland, Kina och Iran. Dessa hotaktörer utgör på olika sätt hot mot svensk elförsörjning. Detta givet att de har olika intressen, mål och tillvägagångssätt. En utveckling som dock har kunnat skönjas, och som de senaste åren har intensifierats, är att flera stater som bedöms utgöra hot mot Sverige och västvärlden samverkar och förstärker varandra. Skiljelinjen mellan hotaktörer kan därför vara diffus.

Några exempel på detta under de senaste åren är bland annat iranskt och kinesiskt stöd till Rysslands krigföring i Ukraina samt Rysslands användande av Kina och Iran som mellanhänder för att kringgå sanktioner och få tillgång till teknik och varor, exempelvis teknologi med dubbla användningsområden. Under 2025 tecknade även Ryssland och Iran ett avtal på säkerhets- och försvarsområdet.

Den organiserade brottsligheten utgör ett hot mot elförsörjningens aktörer, både i sig själv och som möjligt ombud för främmande makt. Våldsbejakande extremistgrupper har hittills inte utgjort ett hot mot svensk elförsörjningen specifikt, men det kan inte uteslutas att vissa grupperingar skulle kunna tänkas göra det framöver. Dessutom föreligger en risk att personer i våldsbejakande extremistiska rörelser används som ombud av främmande makt.

De statliga hotaktörerna samt organiserad brottslighet och våldsbejakande extremism redogörs för nedan utifrån deras relevans för

svensk elförsörjning. För en mer djupgående beskrivning av hotaktörerna hänvisas till försvars- och underrättelsemyndigheternas publikationer.

3.3.1 Ryssland

Enligt Säkerhetspolisen är Ryssland fortsatt det största hotet mot Sverige, och Svenska kraftnät delar den bedömningen när det kommer till svensk elförsörjning. Vidare beskriver Säkerhetspolisen hur Ryssland, sedan deras fullskaliga invasion av Ukraina, är mer riskbenäget och opportunistiskt även utanför konfliktområdet. Det svenska Nato-inträdet har stärkt Sveriges säkerhet men samtidigt inneburit ett ökat underrättelseintresse gällande svenska militära förmågor och kritisk infrastruktur, inklusive anläggningar, system och funktioner inom elförsörjningen.

De ryska underrättelse- och säkerhetstjänsterna använder informationspåverkan i syfte att påverka västvärldens stöd för Ukraina och för att öka polariseringen. Rysslands hybrida aktiviteter i form av påverkansoperationer och sabotage har intensifierats och flera länder har under 2025 pekat ut Ryssland som ansvarigt för sådana aktiviteter. En metod som förekommer mer frekvent för sabotageverksamhet är användandet av förbrukningsagenter. Förbrukningsagenter är personer som rekryteras, inte sällan i den digitala miljön och med pengar som motivation, för att utföra enstaka uppdrag. Att använda förbrukningsagenter är också ett sätt att öka möjligheten till förnekbarhet från rysk sida.

För elförsörjningen innebär ryska hybridaktiviteter en risk för fysisk skadegörelse mot anläggningar samt cyberangrepp, informationspåverkan och underrättelseinhämtning riktad mot kritisk verksamhet inom sektorn.⁷

3.3.2 Kina

Säkerhetspolisen bedömer att Kina fortsatt utgör det långsiktiga hotet mot Sveriges ekonomiska säkerhet. Kinas mål är att långsiktigt kontrollera och dominera frågor som världshandel och ekonomi. Till sin hjälp för att uppnå sina säkerhetspolitiska mål har den kinesiska staten hela samhällets resurser, både genom lagliga och olagliga metoder.

⁷ Säkerhetspolisen (2026), *Lägesbild 2025-2026*.

Den säkerhetshotande verksamhet som kinesisk underrättelse- och säkerhetstjänst bedriver i Sverige riktas främst mot ekonomiska förbindelser, teknik och kunskap. Syftet med detta är att stärka Kinas inhemska förmåga och kunskap inom olika områden eller att skapa beroenden. Detta övertag kan sedermera användas i påverkanssyfte. Detta kan exempelvis ske genom olika former av investeringar och äganden. Kina har ett särskilt intresse av skyddsvärd verksamhet, kring svenska företag, universitet, forskare och andra experter, inkluderat sådana som är verksamma inom eller runt elförsörjningen.

Ett annat tillvägagångssätt som den kinesiska underrättelse- och säkerhetstjänsten använder sig av för att komma över kunskap och teknik är cyberangrepp. Kina använder sig även av kinesiska medborgare och företag för sin underrättelseinhämtning, vilket den kinesiska underrättelselagen från 2017 ett exempel på. Underrättelselagen har långtgående konsekvenser för hur individer och organisationer ska samverka med den kinesiska staten. Allra tydligast regleras detta i artikel 7, i vilken det stipuleras att alla organisationer och medborgare ska stödja, hjälpa och samarbeta med underrättelsetjänsten.⁸

För svensk elförsörjning är Kinas säkerhetshotande verksamhet främst relevant genom underrättelseinhämtning riktad mot teknik, information, industriella processer och expertis.

3.3.3 Iran

Den senaste tidens händelseutveckling i Iran i form av USA:s och Israels militära operation i landet försvårar bedömningen av vilket hot Iran kommer att utgöra framöver, eftersom det är avhängigt det framtida styret i landet.

Säkerhetshotande verksamhet som Iran bedriver i Sverige är flyktingspionage och påtryckning samt kartläggning av oppositionella i den iranska diasporan, försök att kringgå sanktioner för att komma åt teknik och forskning, inte minst kopplat till sitt kärnvapenprogram, samt användande av kriminella nätverk som ombud för att begå våldsdåd mot israeliska och judiska mål.⁹

⁸ Nationellt kunskapscentrum om Kina, "Kinas underrättelselag: konsekvenser för individer och företag", Kinas underrättelselag: konsekvenser för individer och företag - Swedish National China Centre, publicerad 2025-10-21.

⁹ Ibid.

Det iranska hotet mot svensk elförsörjning är inte styrkt i samma utsträckning som det ryska och kinesiska. Däremot bedriver Iran säkerhetshotande verksamhet i Sverige och har dokumenterat använt sig av ombud på svensk mark och har således en sådan förmåga. I dagsläget finns det emellertid inga indikationer på att iransk ombudsverksamhet skulle rikta sig mot svensk elförsörjning. Beträffande det iranska underrättelsehotet kan det inte uteslutas att iranska underrättelser, exempelvis avseende svensk elförsörjning, delas med andra intressenter så som Ryssland och Kina.

3.3.4 Organiserad brottslighet

Den organiserade brottsligheten har historiskt sett handlat om exempelvis gängkriminalitet, narkotikahandel, bedrägerier och ekonomisk brottslighet. Numera handlar det också i allt större utsträckning om bland annat olika former av cyberkriminalitet, välfärdsbrottslighet (där kriminella utnyttjar välfärdssystemen), mutbrott, samt avancerade internationella upplägg i den kriminella ekonomin. För elförsörjningen är det särskilt tre olika typer av hot med koppling till organiserad brottslighet som bedöms vara relevanta: ombud åt främmande makt, cyberkriminalitet och materielstölder.

3.3.4.1 Ombud

Personer inom den organiserade brottsligheten kan användas som ombud av främmande makt. Motivet bakom detta är ekonomiska, där uppdrag utförs mot pengar. Det är inte heller säkert att uppdragstagaren är medveten om att det är främmande makt som är anstiftare.

Främmande makts verksamhet via ombud omfattar dock inte enbart personer inom den organiserade brottsligheten. Övriga kan vara icke-kriminella, icke-organiserade kriminella, personer inom våldsbejakande extremistiska rörelser (se nedan under 3.3.5) eller personer med missbruksproblematik.¹⁰ Från Ukraina rapporteras det även om personer som via sociala plattformar, exempelvis TikTok och spelplattformar, rekryteras av ryska säkerhetstjänster för att utföra uppdrag mot pengar (så kallade förbrukningsagenter). Det rör sig inte sällan om enstaka uppdrag där uppgiften kan vara av enklare slag.¹¹

¹⁰ Svenska Yle, "Skypo om misstänkta sabotage i Europa: Ryssland använder mellanhänder", <https://yle.fi/a/7-10074523>, publicerad 2025-03-17.

¹¹ International Centre for Counter-Terrorism, "More of the Same. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited", [More of the Same. Russia's Crime-Terror](#)

3.3.4.2 Cyberkriminalitet

Cyberkriminalitet kan vara drivet av ekonomiska intressen eller aktivistiska och/eller politiska mål. Det förra sker inte sällan i form av utpressningsattacker där en hotaktör använder ransomware för att låsa ett system och/eller komma över data och sedan vill ha betalt för att låsa upp systemet eller för att inte publicera den stulna datan. Det senare kan vara i form av så kallad hacktivism, där hotaktören drivs av politiska mål eller av att helt enkelt försöka hitta svagheter. Cyberkriminella grupperingar kan antingen verka självständigt eller som ombud för främmande makt.

Det finns en mängd olika aktiva kriminella grupperingar som utför cyberangrepp som tjänst (crime as a service) och de riktar ofta in sig på olika delar av cyberangrepps-kedjan och säljer information och verktyg till varandra. Denna utveckling inom cyberkriminalitet driver på ett professionaliserat kriminellt ekosystem som i slutändan gör det svårt för en verksamhetsutövare att identifiera vem angriparen är.¹²

3.3.4.3 Materielstölder

Den organiserade brottsligheten kan även drabba infrastruktur genom fysiska stölder. Framförallt sker det genom kopparstölder, exempelvis från kraftstationer eller järnvägsanläggningar. Kopparstölder har ökat under de senaste åren, bland annat med anledning av att värdet på koppar har ökat. Stölder av koppar, bränsle, reservdelar, verktyg och annan väsentlig utrustning kan påverka tillgängligheten i elförsörjningen samt påverka återställningsförmågan.

3.3.5 Våldsbejakande extremism

I Nationellt centrum för terrorhotbedömning (NCT) helårsbedömning för 2026 lyfts statlig förnekbar våldsförmåga via nyttjande av ombud. För att främja sina strategiska mål använder sig vissa aktörer av ombud för att utföra förnekbara våldshandlingar i andra länder. I vissa fall är ombuden dessutom omedvetna om vem anstiftaren egentligen är och vad denna har för syften. Exempel på detta är hur ryska statsaktörer, med hjälp av ombud, har bedrivit sabotageverksamhet i Europa kopplat till stödet till Ukraina.¹³

Nexus: Criminality as a Tool of Hybrid Warfare Revisited | International Centre for Counter-Terrorism - ICCT, publicerad 2026-02-23.

¹² Dragos, *Year in review -OT/ICS cybersecurity report*, publicerad februari 2026.

¹³ Nationellt centrum för terrorhotbedömning (2026), *Helårsbedömning 2026*.

NCT skriver att aktörerna bakom flera av de fall i västvärlden där högerextremistiskt motiverade terrorattentat genomförts eller avvärjts har hänvisat till, konsumerat och spridit accelerationistisk propaganda. Propagandan uppmanar till våldshandlingar riktade mot samhället, systemet i stort eller minoritetsgrupper med det bakomliggande syftet att påskynda en samhällskollaps som sedan ska möjliggöra upprättandet av ett etniskt homogent samhälle. Accelerationism kan beskrivas som en politisk strategi som bygger på grundtanken att samhällsutvecklingen är predestinerad mot undergång, och att denna undergång kan påskyndas för att ersätta samhällssystemet med vad de anser vara ett idealsamhälle.¹⁴

Ett exempel är ekofascism som Totalförsvarets forskningsinstitut (FOI) beskriver i en studie från 2020 som en typ av en accelerationistisk rörelse, där just det accelerationistiska inslaget anses nödvändigt för att rädda jordens ekosystem.¹⁵ Högerextrema våldshandlingar riktade mot just svensk elförsörjning har inte förekommit men det finns emellertid exempel från USA där sådana handlingar har riktats mot elförsörjningen.¹⁶

Center mot våldsbejakande extremism (CVE) lyfter i en rapport från 2021 om högerextrem accelerationism det svenska fallet från 2020 där två unga män åtalades för att ha utfört en mordbrand mot en minkfarm i Sölvesborg. I samma rapport konstateras att högerextrem accelerationism har potential att inspirera både celler och ensamagerande att utgöra våldsdåd i Sverige. Att den accelerationistiska rörelsen är löst sammansatt medför också att det föreligger en risk att främmande makt kan infiltrera och utnyttja den i syfte att uppnå sina mål.¹⁷

Det finns även under de senaste åren exempel där vissa miljö- och klimataktivistiska rörelser har ägnat sig åt fysiska aktioner mot infrastruktur, inklusive infrastruktur inom elförsörjningen. Några sådana europeiska exempel är Extinction Rebellions blockad mot gasterminalen på Kårstø i Norge (2024)¹⁸, franska anarkistgrupper som tog på sig två sabotage mot elnätet (i form av anlagda bränder i kraftstationer) i södra

¹⁴ Center mot våldsbejakande extremism, *Våldsbejakande högerextrem accelerationism*, publicerad januari 2021.

¹⁵ Totalförsvarets forskningsinstitut, *Ekofascism – En studie av propaganda i digitala miljöer*, publicerad 2020-12-21.

¹⁶ Combating Terrorism Center, *From Earth Liberation to Accelerationism: A High-Level Review of Fifty Years of Domestic Infrastructure Terrorism*, publicerad mars 2026.

¹⁷ Center mot våldsbejakande extremism, *Våldsbejakande högerextrem accelerationism*, publicerad januari 2021.

¹⁸ NRK Rogaland, "Slo til med storaksjon mot gassanlegg lørdag – nå vil de forstyrre energimesse", *Extinction Rebellion med rekordvekst etter NRK-serie. Vil forstyrre ONS, verdens største energimesse – NRK Rogaland – Lokale nyheter, TV og radio*, publicerad 2024-08-24.

Frankrike (2025)¹⁹ och det löst sammansatta vänsterextrema nätverket Vulkangruppe som har tagit på sig flera sabotage mot Tysklands infrastruktur, bland annat under 2026.²⁰

Våldsbejakande islamistiska aktörer har historiskt främst riktat sina attentat mot civila och symboliska mål snarare än kritisk infrastruktur. Det finns inte heller några exempel där svensk elförsörjning varit föremål för angrepp från våldsbejakande islamism. Även om svensk elförsörjning inte bedöms utgöra ett av de mest troliga målen för angrepp från våldsbejakande islamistiska aktörer kan det inte uteslutas att elförsörjningen kan vara ett potentiellt mål om ett sådant angrepp skulle bedömas bidra till aktörens strategiska syften.

En utveckling inom extremistmiljöerna som Säkerhetspolisen ser är att våldsutövandet kan vara ett mål i sig. Detta innebär att våldet kan vara överordnat drivkrafterna, vilket innebär att det är mer sannolikt att individer rör sig mellan olika våldsbejakande grupper.²¹ Det saknas kända exempel på angrepp mot svensk elförsörjning från våldsbejakande extremistiska grupper. Däremot finns det internationella exempel där infrastruktur inom elförsörjningen varit föremål för sabotage eller störningsaktioner. De våldsbejakande extremistiska grupperna är inte sällan löst sammansatta och internationella till sin natur.

Det kan inte uteslutas att svensk elförsörjning kan utgöra ett attraktivt mål för våldsbejakande extremistiska aktörer, däribland högerextrema accelerationister, vänsterextrema eller våldsbejakande islamister, eftersom sabotage och störningar kan få stora samhällskonsekvenser, skapa uppmärksamhet, bidra till misstro eller uppfattas vara ett medel för att uppnå ideologiska mål. Vidare kan våldsbejakande extremistiska grupper medvetet eller omedvetet användas som ombud av främmande makt för att uppnå dess mål.

3.4 Mål inom elförsörjningen

Tänkbara mål inom elförsörjningen kan variera beroende på hotaktör och underliggande avsikt. Det kan vara mål med betydelse för Sveriges säkerhet och som omfattas av säkerhetsskyddslagstiftningen, men det kan också vara mål som inte har direkt betydelse för Sveriges säkerhet,

¹⁹ Omni, "Strömlöst på rivieran efter nytt misstänkt sabotage", Strömlöst på rivieran efter nytt misstänkt sabotage, publicerad, publicerad 2025-05-25.

²⁰ Omni, "Polisen i Tyskland jagar extremt vänsternätverk", Polisen i Tyskland jagar extremt vänsternätverk, publicerad 2026-05-11.

²¹ Säkerhetspolisen (2026), *Lägesbild 2025-2026*.

men som icke desto mindre är av betydelse för aktören och andra som blir drabbade.

En kategorisering kan göras över tänkbara mål inom elförsörjningen utifrån varför ett visst mål är betydelsefullt, det vill säga på vilket sätt ett angrepp kan åsamka skada. I det avseendet kan de perspektiv som används inom säkerhetsskyddsområdet – konfidentialitet, riktighet och tillgänglighet – vara till hjälp. Nedan ska inte ses som en uttömmande lista över tänkbara mål utan utgör endast exempel på vissa typer av tänkbara mål samt hur de kan sorteras.

Det är viktigt att notera att samtliga mål som redogörs för nedan antingen kan finnas i egen regi hos aktörer själva eller hos externa leverantörer i leveranskedjor.

3.4.1 Konfidentialitet

Att någonting är betydelsefullt ur ett konfidentialitetsperspektiv innebär att skada uppstår om ett röjande sker. Detta kan vara information om sårbarheter, exempelvis kopplat till IT- eller OT-system, men också om anläggningar, processer, förmågor, reservplaner, reservdelar, leveranskedjor, totalförsvarsplanering samt annat där ett röjande av informationen kan innebära att skada uppstår. Det som utmärker denna typ av mål är att det är själva informationen som är det betydelsefulla. En antagonist är intresserad av denna typ av mål för att tillägna sig antingen kort- eller långsiktiga fördelar. Informationen kan bland annat användas för att underlätta framtida angrepp, exempelvis genom sabotage, informationspåverkan, cyberangrepp eller ytterst krigsförberedelse.

3.4.2 Riktighet

Att något är betydelsefullt ur ett riktighetsperspektiv innebär att skada uppstår till följd av att någonting manipuleras. Manipulation kan exempelvis ske av OT-system eller system och utrustning som finns till för att skydda olika komponenter. Manipulation kan även ske av data som är avgörande för olika typer av beslutsfattande inom elförsörjningen. Detta kan vara data som är avgörande för operativa och tidskristidskritiska beslut eller data som är betydelsefull för att fatta strategiska och långsiktiga beslut. Skada utifrån riktighet kan leda till oförutsägbarhet och försämrad funktionalitet eftersom otillförlitlighet leder till ovisshet. I värsta fall kan skada utifrån riktighet även leda till att skada uppstår i form av förlorad tillgänglighet, se nedan.

3.4.3 Tillgänglighet

Att något är betydelsefullt ur ett tillgänglighetsperspektiv innebär att skada uppstår till följd av att någonting inte kan komma åt när och där det behövs då det gjorts otillgängligt. Detta kan antingen vara otillgängliggörande av OT-system, data eller fysisk utrustning, exempelvis olika typer av produktions- och distributionsanläggningar eller komponenter på dessa. Skada utifrån tillgänglighet kan orsakas genom riktighetsskador, det vill säga att manipulation av något leder till ett otillgängliggörande. Exempel på det kan vara att oriktig information leder till felaktiga beslut i operativ verksamhet, som därmed orsakar en förlorad tillgänglighet. Andra sätt som skada utifrån tillgänglighet kan orsakas är genom att något exempelvis stängs ned, saboteras, krypteras eller på annat sätt görs otillgängligt.

3.4.4 Andra typer av mål

Det finns även tänkbara mål inom elförsörjningen som inte på något enkelt sätt kan sorteras under perspektiven konfidentialitet, riktighet och tillgänglighet. Ett sådant mål är personal. Personal inom elförsörjningen är ett tänkbart mål såtillvida att personalen skulle kunna användas som medel för att komma åt andra typer av mål, exempelvis sådana som nämnts ovan – information om sårbarheter, IT- eller OT-system, fysiska anläggningar eller för att påverka operativt eller strategiskt beslutsfattande. Detta kan ske genom exempelvis hot och våld, mutor, identitetsstöld, stöld av passerkort eller IT-utrustning, värvningsförsök (insiders) eller phishing.

Ett annat sådant mål är vad som skulle kunna beskrivas som förtroende eller tillit till aktörer inom elsektorn. Attacker mot förtroende kan syfta till att antingen generellt, eller i specifika frågor, minska tilliten till aktörer inom elförsörjningen, och således öka polariseringen. En ökad polarisering och ett minskat förtroende genom informationspåverkan kan även öka risken för att exempelvis krisinformation misstros.

Ytterligare ett mål som inte främst kretsar kring konfidentialitet, riktighet och tillgänglighet är mål av ekonomiska värden. Detta rör olika typer av materiel som finns hos aktörer inom elförsörjningen och som löper risk för att stjälas. Detta kan emellertid få konsekvenser för exempelvis tillgängligheten om det rör stöld av komponenter som då inte finns tillgängliga när de behövs.

3.5 Hotbildens föränderlighet och vad det medför

Svenska kraftnät vill särskilt understryka att hotbilden kan se olika ut beroende på vilket mål som avses. Olika antagonistiska aktörer kan ha olika motiv och metoder beroende på vilka mål de riktar in sig på och vilka syften de vill uppnå.

En aktörs avsikt kan snabbt förändras, vilket gör att hotbilder är en färskvara. Svenska kraftnät uppmanar därför aktörer verksamma inom elförsörjningen att bevaka uttalanden från myndigheterna inom underrättelseområdet, exempelvis Säkerhetspolisen och FRA. Verksamhetsutövare inom elförsörjningen bör också vara vaksamma på lägesbilden för sin egen verksamhet. Fokus behöver ligga på vad som utgör vardag, den så kallade normalbilden, och vad som avviker från denna. Vid säkerhetshotande och anmälningspliktiga händelser enligt 2 kap 4 § säkerhetsskyddsförordningen (2021:955) ska dessa anmälas till Säkerhetspolisen. Information och anmälningar till Säkerhetspolisen är avgörande för att Säkerhetspolisen ska kunna upprätthålla och förbättra sin lägesbild gällande hoten mot Sverige, inklusive mot elförsörjningen.

De antagonistiska aktörernas förmåga varierar, och som nämnts i tidigare kapitel samarbetar också dessa aktörer. För säkerhetskänslig verksamhet ansvarar Säkerhetspolisen för att styra dimensioneringen av det fysiska skyddet genom sin publikation Dimensionerande antagonistiska förmågor (DAF). Publikationen delges de verksamheter som har säkerhetskänslig verksamhet, utifrån den grad av skada som ett angrepp mot verksamheten kan få, se nivåerna i 2 kap 5 § säkerhetsskyddslagen (2018:585) samt i 2 kap 5 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1).

4 Antagonistiska hot

4.1 Cyberhot

Det främsta hotet avseende cyberangrepp bedöms komma från främmande makt och organiserad brottslighet, särskilt med anledning av det försämrade säkerhetspolitiska läget. Att pågående krig och konflikter runt om i världen sprider sig till cyberdomänen visar sig i att många av de angrepp som skett på senare år kan kopplas till geopolitik.²² Exempelvis har överbelastningsangrepp skett som svar på olika typer av symboliska handlingar, som löften och beslut om stöd till Ukraina i det pågående försvarskriget mot Ryssland.

Av Myndigheten för civilt försvars cyberincidentrapportering 2025 framgår att överbelastningsangrepp är angreppsmetod som rapporterats mest av de myndigheter och organisationer som är ålagda att rapportera cyberincidenter enligt lag.²³ Även ENISA rapporterar att överbelastningsangrepp står för merparten av de rapporterade incidenterna och pekar särskilt ut angrepp med koppling till geopolitiska motiv där statliga aktörer och kritisk infrastruktur är måltavlor.²⁴ Samtidigt har det skett en ökning av så kallade "wiper-attacks", där skadlig kod används för att permanent radera och förstöra data.²⁵ Ökningen visar på att cyberangrepp allt oftare används som strategiska störnings- och påverkansmedel inom ramen för hybridaktiviteter.

Inom cyberhot märks även en ökad hotbild specifikt mot OT-system. MCF rapporterar att angreppen mot OT-system har ökat under perioden 2023-2025. Det kan dels handla om utpressningsangrepp men även angrepp med rent destruktiva syften, det vill säga att med hjälp av OT-specifik skadlig kod radera eller förstöra information för att åstadkomma reella störningar och otillgängliggöra systemen helt och hållet. Även vid dessa angrepp finns ofta en koppling till geopolitiska konflikter och de riktas mot flera olika samhällssektorer, däribland energisektorn och statliga aktörer.

²² Myndigheten för civilt försvar (MCF), *Cyberangreppens utveckling 2023-2025 – Årsrapport cyberincidentrapportering 2025*, MCF0108, publicerad mars 2026.

²³ Myndigheten för civilt försvar (MCF), *Cyberangreppens utveckling 2023-2025 – Årsrapport cyberincidentrapportering 2025*.

²⁴ European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2025*, publicerad oktober 2025.

²⁵ Dragos (2026), *Year in review -OT/ICS cybersecurity report*.

Denna utveckling kan ses till följd av en ökad sammankoppling mellan IT- och OT-miljöer samt fler fjärranslutningar till dessa.²⁶

Cyberangrepp kan genomföras både för underrättelseinhämtning (cyberspionage) och för att skapa möjligheter till framtida angrepp. Genom att etablera en så kallad vilande närvaro i ett IT-system kan en angripare samla in information, kartlägga system eller plantera skadlig kod som kan användas vid ett senare angrepp. Till skillnad från ett direkt cyberangrepp är syftet att en sådan operation inte ska märkas alls. Ett exempel på detta är den attack som utfördes mot transmissionsnätet i Ukraina 2015. Ryssland har även därefter fortsatt med cyberspionage i ukrainska nätverk och utnyttjat detta sedan den fullskaliga invasionen 2022.²⁷

Utöver ett omfattande beroende av tekniska system har många verksamheter även ett beroende av satellittjänster för att de tekniska systemen ska fungera. Tid och frekvens via globala satellitnavigeringssystem (GNSS) är exempel på sådana satellittjänster. Det innebär att påverkan på GNSS, exempelvis GPS, kan medföra störningar hos tekniska system som i sin tur påverkar aktörer och deras uppdrag. Transportstyrelsen rapporterade i september 2025 en kraftig ökning av GPS-störningar i Östersjön, både i omfattning och rent geografiskt.²⁸ Dessa störningar påverkar fortsatt såväl sjö- som luftfartstrafik.

4.1.1 AI:s betydelse för cyberhotbilden

Hotaktörer inom cyberområdet har idag en generellt hög förmåga att genomföra komplexa cyberangrepp, där kritisk infrastruktur utgör en måltavla. Med hjälp av AI har metoderna för cyberangrepp blivit mer sofistikerade och avancerade. Exempelvis används AI för att effektivisera metoder som nätfiske plantering av skadlig kod och för att genomföra angrepp i större skala än tidigare. AI används också som ett verktyg för social manipulation, exempelvis genom röstkloning.²⁹ Utvecklingen innebär att grupper som tidigare saknat resurser eller tekniska kunskaper istället kan använda AI som verktyg. Sannolikt kan detta driva på en

²⁶ European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2025*

²⁷ Myndigheten för civilt försvar (2026), *Cyberangreppens utveckling 2023-2025 – Årsrapport cyberincidentrapportering 2025*.

²⁸ Transportstyrelsen, "Kraftig ökning av GPS-störningar i Östersjön", <http://www.transportstyrelsen.se/sv/om-oss/pressrum/nyhetsarkiv/2025/kraftig-okning-av-gps-storningar-i-ostersjon/>, publicerad 2025-09-04.

²⁹ CERT-EU, *Threat landscape Report 2025: A year in review*, publicerad 2026-04-08

ökning av utpressningsangrepp från kriminella aktörer som söker ekonomisk vinning.

AI används även för att identifiera sårbarheter och möjliga angreppsvektorer. I april 2026 tillkännagav företaget Anthropic en ny modell med förmåga att självständigt identifiera och exploatera sårbarheter i programvara. Modellen har på egen hand och under några veckors tid upptäckt tusentals kritiska sårbarheter i flera olika operativsystem. Modellen bedöms vara så kapabel att Anthropic själva valde att initialt inte tillgängliggöra den, då de identifierade sårbarheterna potentiellt skulle kunna utnyttjas av en antagonist. Istället initierades projektet Glasswing där utvalda aktörer får tillgång till programvaran för att identifiera och åtgärda sårbarheter i sina egna system.³⁰

Modellen som beskrivs ovan är bara ett exempel på AI:s betydelse för det växande cyberhotet och att cybersäkerhetsarbetet står inför stora utmaningar vad gäller att möta denna typ av hot.³¹

4.1.2 Aktuella händelser

I april 2025 drabbades en dammanläggning i Bremanger, Norge, av ett cyberangrepp mot styrsystemet som möjliggjorde för angriparna att öppna dammportarna under fyra timmar. Enligt den norska säkerhetspolisen PST låg pro-ryska aktörer bakom händelsen.³²

Under våren 2025 ska ett värmeverk i västra Sverige ha utsatts för ett försök till cyberangrepp. En pro-rysk hacktivistgrupp ska ha legat bakom det misslyckade försöket.³³

I oktober 2025 drabbades Svenska Kraftnät av ett dataintrång där en hackergrupp fick åtkomst till data via en extern och avgränsad

³⁰ Anthropic, "Project Glasswing: Securing critical software for the AI era", <https://www.anthropic.com/glasswing>.

³¹ AI Security Institute (AISA), "Our evaluation of Claude Mythos Preview's cyber capabilities", <https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities>, publicerad 2026-04-12.

³² VG, "PST-sjefen mener pro-russiske hackere sto bak cyberangrepet mot damanlegget i Bremanger", <https://www.vg.no/nyheter/i/mPJaE4/pst-sjefen-mener-pro-russiske-hackere-sto-bak-cyberangrepet-mot-damanlegget-i-bremanger>.

³³ SVT Nyheter, "Prorysk hackerattack mot Sverige – misslyckades", <https://www.svt.se/nyheter/inrikes/regeringen-om-cyberhotet-mot-sverige>, publicerad 2026-04-15.

filöverföringstjänst.³⁴ Hackergruppen Everest, har senare tagit på sig ansvaret för attacken.

I december 2025 riktades flera omfattande cyberattacker mot Polens energisektor, bland annat drabbades flera vind- och solkraftanläggningar och ett värmekraftverk. Händelsen visar på ett angreppsätt där attacker riktades mot såväl IT- som OT-system samtidigt med syfte att förstöra information snarare än att stjäla den. De polska myndigheterna drar slutsatsen att de koordinerade attackerna utfördes av en och samma antagonist.³⁵ Angreppets karaktär utgör en tydlig eskalering i den ryska hybridkrigföringen i den mening att den även riktar sig mot kritisk infrastruktur bortom Ukraina och mot system i länder som stödjer Ukraina.

4.2 Fysisk skadegörelse och sabotage

Sabotage är en form av fysisk skadegörelse som syftar till att försämra förmågan hos den angripna verksamheten att upprätthålla sin funktionalitet. Syftet kan också vara att testa förmågan till upptäckt och hantering av sabotage och ske i förberedande syfte som ett led i hybridkrigföring. För verksamheter inom elförsörjningen kan det handla om förstörelse av fysiska delar på produktionsanläggningar eller distributionsanläggningar eller i IT-/OT-infrastruktur. Det kan även handla om cyberangrepp som kombineras med fysiskt sabotage av utrustning.

Det förekommer ideologiskt motiverade brott (framförallt skadegörelse) som begås utifrån politiska skäl eller religiös övertygelse och kan vara kopplat till en konflikt, en sakfråga eller en situation som uppfattas som orättvis (se även avsnitt 3.3.5). Inom elförsörjningen så har historiskt sett kärnkraften varit måltavla för denna typ av antagonister men hotbilden riktar sig även mot andra typer av energislag, exempelvis fossildrivna sådana.³⁶

Även missnöje med att mark används för elförsörjningens infrastruktur (t.ex. ledningar och ledningsstolpar) kan yttra sig i försök till fysisk skadegörelse och stöld.

³⁴ Svenska kraftnät, "Samlad information om dataintrånget", <https://www.svk.se/sakerhet-och-beredskap/cybersakerhet/samlad-information-om-dataintranget/>.

³⁵ CERT Polska, *Energy sector incident report – 29 december*, publicerad 2026-01-30.

³⁶ SVT Nyheter, "Tiotusentals utan ström i Berlin – vänsterextrem grupp tar på sig ansvaret", <https://www.svt.se/nyheter/utrikes/tiotusentals-utan-strom-i-berlin>, publicerad 2026-01-03.

Elförsörjningens anläggningar, eller byggarbetsplatser för sådana, innehåller också stöldbegärlig egendom som explosivämnen, metaller, verktyg och maskiner, vilket gör att inbrott och stölder förekommer. Även kopparkabel utanför anläggningarna kan vara stöldbegärliga, trots att det för tjuven kan vara förenat med livsfara att genomföra stölden. Motiven för sådana stölder är sällan att sabotera eller förstöra utrustning utan snarare ekonomisk vinning. Trots detta kan stölder medföra konsekvenser som i praktiken liknar dem som uppstår vid sabotage eller skadegörelse, eftersom stulen eller skadad utrustning kan orsaka störningar och försämrad leveransförmåga.

4.2.1 Aktuella händelser

Stölder och inbrott kopplade till elförsörjningen sker återkommande runt om i landet. Oftast som ovan nämnt för att få tillgång till materiel som är enkelt att sälja vidare. Bland annat drabbades ett ställverk i Östergötland av inbrott i februari 2024 och flera transformatorer slogs sönder. Tre personer dömdes i augusti samma år för bl.a. grov skadegörelse.³⁷

Frågor kring upplåtelse av mark för uppförande av kraftledningar kan väcka missnöje och leda till skadegörelse. I augusti 2024 kapades ett antal kraftledningsstolpar med motorsåg i södra Halland. En anmälan om skadegörelse upprättades med lades senare ned då ingen misstänkt kunde identifieras.³⁸

I januari 2026 utsattes ett vattenverk i Västerås för ett sabotage som ledde till strömbrott när en obehörig person tog sig in i ett ställverk och slog av strömmen.³⁹

I januari 2026 blev ca 45 000 hushåll strömlösa i Berlin, Tyskland, när flera högspänningsledare nära ett kraftverk förstördes i en anlagd brand. Även det lokala värmenätet liksom mobilnät och kollektivtrafik påverkades. Den vänsterextrema Vulkangruppe tog i efterhand på sig

³⁷ SVT Nyheter, "Trio döms till fängelse för sabotage av skyddsobjekt i Östergötland", <https://www.svt.se/nyheter/lokalt/ost/trio-doms-till-fangelse-for-sabotage-av-skyddsobjekt-i-ostergotland>, publicerad 2024-08-06.

³⁸ SVT Nyheter, "Utbrett sabotage av kraftledningar i södra Halland – kapade med motorsåg", <https://www.svt.se/nyheter/lokalt/halland/utbrett-sabotage-av-kraftledningar-i-sodra-halland-kapade-med-motorsag>, publicerad 2024-08-29.

³⁹ Mälarenergi, "Nya säkerhetsåtgärder efter sabotage mot vattenverk", <https://www.malarenergi.se/om-malarenergi/malarenergi/pressrum/#/embedded/release/4255358/nya-sakerhetsatgarder-efter-sabotage-mot-vattenverk?publisherId=3236664&lang=sv>, publicerad 2026-02-19.

ansvaret för aktionen som angavs vara riktad mot den fossila bränsleindustrin.⁴⁰

I tidigare version av denna hotbild från 2024 uppmärksammades sprängdåden mot gasledningarna NordStream 1 och 2 i Östersjön i september 2022 liksom en läcka på en undervattensledning för gas i Finska viken 2023. Flera händelser har sedan dess uppmärksammats där det uppstått skador på undervatteninfrastruktur i Östersjön, framförallt rör det sig om skador på kommunikations- och datakablar.

Bland annat upptäcktes skador på fyra undervattenskablar mellan Finland och Estland i december 2024. Ett fartyg tillhörande den ryska skuggflottan misstänktes vara inblandat och tre personer ur besättningen åtalades misstänkta för bland annat grov skadegörelse. I oktober 2025 meddelades att Helsingfors tingsrätt att åtalet avvisades eftersom händelsen skedde på internationellt vatten.⁴¹

Även en kommunikationskabel mellan Sverige och Lettland skadades i januari 2025 men Säkerhetspolisen meddelade i oktober samma år att förundersökningen om grovt sabotage lades ner då det kunde konstateras att det var en olyckshändelse.⁴² Senare i december 2025 upptäcktes också dubbla kabelbrott på en kommunikationskabel mellan Sverige och Estland.⁴³

4.3 Informationsinsamling

Med en ökad generell hotbild mot Sverige blir även underrättelsehotet mer påtagligt. Säkerhetspolisen pekar på att främst Kina och Ryssland har en aktiv informationsinsamling om säkerhetskänslig verksamhet i Sverige och det rör sig även om civila mål som kritisk infrastruktur. Antagonistisk underrättelseverksamhet utgör en viktig komponent för hybridaktiviteter och kartläggning av system, reservrutiner, personal och leverantörskedjor bedöms vara av särskilt intresse för en antagonist. Informationsinsamling

⁴⁰ SVT Nyheter, "Tiotusentals utan ström i Berlin – vänsterextrem grupp tar på sig ansvaret", <https://www.svt.se/nyheter/utrikes/tiotusentals-utan-strom-i-berlin>, publicerad 2026-01-03.

⁴¹ SVT Nyheter, "Ingen dom efter kabelbrottet i Östersjön – finsk domstol saknar befogenhet", <https://www.svt.se/nyheter/utrikes/ingen-dom-efter-kabelbrottet-i-ostersjon-finsk-domstol-saknar-befogenhet>, publicerad 2025-10-03.

⁴² Säkerhetspolisen, "Förundersökning om grovt sabotage nedlagd", <https://sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2025-10-13-forundersokning-om-grovt-sabotage-nedlagd.html>, publicerad 2025-10-13.

⁴³ SVT Nyheter, "Flera kabelbrott i Östersjön – sabotage utreds", <https://www.svt.se/nyheter/utrikes/kabelbrott-mellan-finland-och-estland>, publicerad 2025-12-31.

kan ske på en rad olika sätt, till exempel via mänskliga kontakter, teknisk inhämtning och cyberspionage samt via publika källor. Kartläggning av skyddsvärda tillgångar inom elförsörjningen kan blotta vilka kritiska beroenden som finns och var en attack skulle göra störst skada.

Genom kontakter med personal eller leverantörer inom elförsörjningen kan en antagonist få tillgång till information av betydelse för elförsörjningen, tillgång till IT-system (t.ex. genom inloggningsuppgifter) och möjlighet att påverka hur personal agerar (till exempel under kriser). I en studie från FOI redogörs för hur metoderna för underrättelseinhämtning via mänskliga källor (HUMINT) utvecklats genom att analysera öppna fall av individer som dömts för spionage i Europa mellan 2008 och 2024⁴⁴. Studien visar på att hotet från den traditionella insidern nu även breddats till att omfatta förbrukningsagenter och icke-expertyper i civila sektorer. De ryska underrättelsemyndigheterna har särskilt påverkats i denna riktning till följd av de massutvisningar av ryska diplomater som skett runt om i Europa med anledning av kriget i Ukraina.⁴⁵ Nyttjandet av denna typ av okvalificerade utförare gör det samtidigt svårare att koppla hot och aktiviteter till främmande makt.⁴⁶

Även rekryteringsstrategierna har förändrats till att inkludera digitala angreppssätt, till exempel via sociala medier, utöver den klassiska värvningstrappan. Motiven till att låta sig rekryteras utgörs ofta av ekonomiska drivkrafter, ideologiska övertygelser, påtryckningar eller personligt missnöje.⁴⁷

Därutöver har utveckling av AI medfört nya möjligheter för en antagonist att lura, vilseleda och locka anställda eller leverantörer att dela med sig av information om svensk elförsörjning. Genom olika typer av social manipulation kan anställda förmås att lämna ut inloggningsuppgifter eller att omedvetet installera skadlig programvara på IT-utrustning.⁴⁸ Det kan röra sig om nätfiske i form av falska identiteter på sociala medier, AI-genererade deepfakes eller så kallad vishing, en form av nätfiske via

⁴⁴ Elina Elveborg Lindskog, Anna Lioufas och Anna Wagman Kåring, *Spies Among Us: Espionage in Europe – A study on convicted spies in Europe 2008-2024*, Totalförsvarets forskningsinstitut 2026, FOI-R—5866—SE.

⁴⁵ Ibid.

⁴⁶ Försvarsmakten, *MUST årsöversikt 2025*.

⁴⁷ Elveborg Lindskog et al., *Spies Among Us*.

⁴⁸ CERT-EU, *Threat Landscape Report 2025 – A Year In Review*.

telefon. CERT-EU rapporterar en ökning av vishing-angrepp under 2025, vilket indikerar att angriparen aktivt riktar in sig på mänskliga mål.⁴⁹

Informationsinsamling kan även ske genom spaning via drönare, otillåten fotografering och intrång. Därutöver finns också annan så kallad teknisk inhämtning, via exempelvis dataintrång och signalspaning.

Vidare kan informationsinsamling ske via publikt tillgängliga data.⁵⁰ I dag finns det en omfattande tillgång till publika data i form av allmänna handlingar och kommersiellt tillgängliga data från exempelvis karttjänster. För elförsörjningen kan det exempelvis avse öppna data kring elproduktion samt marknadsinformation om balanseringstjänster och kapacitet i nätet. Lägg därtill att ledningsnät och stationer inom elförsörjningen i hög grad utgörs av för allmänheten synliga anläggningar. Denna öppna information kan potentiellt utnyttjas av en antagonist i kartläggningssyfte.

4.3.1 Aktuella händelser

Det mest uppmärksammade fallet i Sverige gällande informationsinsamling på senare år gäller de två bröder som våren 2023 dömdes för grovt spioneri. Enligt domen agerade bröderna på uppdrag av den ryska underrättelsetjänsten.

I januari 2026 häktades en man med kopplingar till Ryssland på sannolika skäl misstänkt för spioneri. Mannen har varit anställd vid Försvarsmakten och enligt åklagaren rör misstankarna brottslighet sedan 2022.⁵¹

Under våren 2026 greps två personer av tyska myndigheter misstänkta för spionage. Personerna ska för Rysslands räkning ha samlat information om ett företag som levererat drönare till Ukraina och utgör ett exempel på den ökade användningen av förbrukningsagenter.⁵²

En kartläggning som publicerade av Sveriges Radio i mars 2026 visar att över 2000 anmälningar om misstänkt brott mot samhällsviktig verksamhet

⁴⁹ Ibid.

⁵⁰ Daniel Eidenskog och Christian Vestlund, *Publika data som riskfaktor – en förstudie om påverkan på informationssäkerhet och säkerhetsskydd*, Totalförsvarets forskningsinstitut 2026, FOI-R—5931--SE.

⁵¹ SVT Nyheter, "Misstänkt spion häktad – förnekar brott", <https://www.svt.se/nyheter/lokalt/stockholm/misstankt-spion-begars-haktad-emx5vz>, publicerad 2026-01-07.

⁵² Euroactiv, "Two suspected of spying for Russia arrested in Germany, Spain", <https://www.euractiv.com/news/two-suspected-of-spying-for-russia-arrested-in-germany-spain/>, publicerad 2026-03-24.

gjordes under 2025. En fjärdedel av dessa rörde inbrott, olaga intrång eller olaglig fotografering av skyddsobjekt.⁵³

4.4 Strategiska uppköp och investeringar

En hotaktör, eller en aktör med kopplingar till en hotaktör, som gör ett strategiskt uppköp, kan ha som syfte att exempelvis underlätta sabotage eller informationsinhämtning. Ett exempel skulle kunna vara ett strategiskt uppköp av mark- och sjöområden eller fastigheter i närheten av fysiska anläggningar av betydelse för elförsörjningen. Genom ett sådant uppköp skulle en hotaktör kunna skaffa sig vad som förefaller vara en legitim närvaro i området, varifrån denne kan inhämta information om exempelvis rutiner, personalrörelser och fysisk utrustning. Detta skulle exempelvis kunna ske genom installation av utrustning för övervakning. Hotaktören skulle också kunna nyttja sin närvaro i området för installation av utrustning för störning.

Även strategiska uppköp av mark- och sjöområden i närheten av broar och vägar som är nödvändiga för att transportera personal eller materiel till anläggningar inom elförsörjningen kan utgöra ett hot såtillvida att det kan användas för att i ett senare skede blockera eller sabotera dessa. Detta hot föreligger också kopplat till exempelvis viktiga kommunikationsnoder för elförsörjningen. Här handlar de främsta hoten om avlyssning och möjligheten att störa viktig kommunikationstrafik för elsystemet.

Ett uppdagande av att en bedömd hotaktör har köpt fastigheter eller mark nära kritisk infrastruktur kan även ha en förtroendeskadlig effekt för den aktör inom elförsörjningen som äger infrastrukturen.

Även strategiska uppköp av, eller investeringar i, företag inom kritisk infrastruktur kan utgöra ett hot. Hotet kan bestå i insyn i, eller påtryckningar mot, verksamheten. Genom delägandeskap eller andra strategiska investeringar kan den utländska aktören få tillgång till känsliga uppgifter om verksamheten och en möjlighet att påverka hur verksamheten styrs. Globaliseringen har medfört att det inte är ovanligt att företag i olika länder är sammankopplade genom ägarskap.

⁵³ Sveriges Radio, "Fler misstänkta brott mot samhällsviktig verksamhet." <https://www.sverigesradio.se/artikel/fler-misstankta-brott-mot-samhallsviktig-verksamhet>, publicerad 2026-03-04.

Lagen (2023:560) om granskning av utländska direktinvesteringar trädde i kraft den 1 december 2023. Lagen gäller för investeringar i skyddsvärd verksamhet som bedrivs av ett aktiebolag, europabolag, handelsbolag, ekonomiska föreningar eller stiftelser som har säte i Sverige. Lagen gäller också för investeringar i sådan skyddsvärd verksamhet som bedrivs i Sverige i ett enkelt bolag eller som enskild näringsverksamhet.⁵⁴ Lagen omfattar inte förvärv av fast egendom. I maj 2026 gavs en utredare i uppdrag att utreda behovet av ändringar i expropriationslagstiftningen för att möjliggöra expropriation av fast egendom när fastighetsinnehavet kan innebära risker för Sveriges säkerhet. Uppdraget ska redovisas senast den 31 mars 2027.⁵⁵

4.4.1 Aktuella händelser

Ett exempel som har varit uppmärksammat de senaste åren beträffande uppköp av mark- och fastigheter är den rysk-ortodoxa kyrkan i Västerås som är belägen i närheten av Västerås flygplats. Kyrkan är finansierad av det ryska statliga kärnkraftsbolaget Rosatom och Säkerhetspolisen har bedömt att den ryska staten använder kyrkan som en plattform i syfte att bedriva underrättelseinhämtning samt annan säkerhetshotande verksamhet i form av påverkan mot Sverige. Säkerhetspolisen har i samverkan med andra myndigheter agerat för att reducera möjligheten för Ryssland att använda kyrkan som plattform för säkerhetshotande aktiviteter.⁵⁶

I sin lägesbild beskriver Säkerhetspolisen att den ryska staten, till följd av att flera ryska underrättelseofficerare med diplomatisk täckmantel utvisats från Sverige, istället har behövt använda andra plattformar för sitt underrättelse- och påverkansarbete. Det kan exempelvis vara organisationer i Sverige med kopplingar till den ryska staten, och den rysk-ortodoxa kyrkan i Västerås kan ses som ett exempel på detta.⁵⁷

Ett annat exempel från 2023 är uppmärksammandet av att en rysk medborgare med affärsintressen i Ryssland låg bakom köpet av en fastighet i närheten av Muskö, där det finns en örlogsbas samt flera hamnar i bergrum.⁵⁸

⁵⁴ 2§ lagen (2023:560) om granskning av utländska direktinvesteringar.

⁵⁵ Dir. Fö2026:00908

⁵⁶ Säkerhetspolisen (2026), *Lägesbild 2025-2026*.

⁵⁷ Ibid.

⁵⁸ Expressen, "Ryske affärsmannen äger tomt – vid Musköbasen",

Beträffande ryskt ägande i Sverige skriver FOI i rapporten *Ryska investeringar och ekonomiska intressen i Sverige från 2022* att det inte finns några uppgifter om att Ryssland har några direkta ägarintressen i svensk kritisk infrastruktur. Ryska företag hade tidigare en viss verksamhet i Karlshamn genom Nord Stream 2, vilken emellertid avslutades 2019.⁵⁹ Under 2025 släppte Acta Publica en fördjupad rapport om svenska bolag med rysk koppling, baserad på FOI:s rapport från 2022.⁶⁰

Ett annat exempel på utländskt ägande inom svensk elförsörjning är kinesiskt ägarskap av svensk vindkraft. Under 2023 bedömdes 10,4 procent av Sveriges installerade vindkraftskapacitet kontrolleras av tre kinesiska statligt ägda företag, vilket motsvarade 3,4 procent av den totala elproduktionen. Detta beskrivs i rapporten *Kinesisk närvaro i den svenska vindkraftssektorn: sårbarheter och risker*. I rapporten bedömdes riskerna med det kinesiska ägandet som relativt låga kopplat till avbrott i elförsörjningen och elprismanipulation. Detta på grund av den begränsade marknadspåverkan och de höga kostnader sådana åtgärder skulle innebära för kinesiska intressen. Det som däremot lyfts fram som ett mer betydande kort- och långsiktigt hot är beroendet av kinesiska leveranskedjor, vilka kan utnyttjas för att exempelvis begränsa tillgången på reservdelar.⁶¹ Detta är inte unikt för vindkraftsbranschen. Ett beroende av kinesiska leveranser och leveranskedjor återfinns i stora delar av samhället, inklusive inom kritisk infrastruktur och elförsörjningen.

Kinesiska och ryska hot i form av strategiska investeringar och utnyttjande av leveranskedjor och beroenden bedöms vara fortsatt aktuella framöver. Dessa hot kan röra olika delar av svensk elförsörjning.

<https://www.expressen.se/nyheter/ryske-affarsmannen-ager-tomt-vid-muskobasen/>, publicerad 2023-01-04.

⁵⁹ Totalförsvarets forskningsinstitut (2022), *Ryska investeringar och ekonomiska intressen i Sverige*.

⁶⁰ Acta Publica (2025), *Ryska intressen – en fördjupad studie av svenska bolag med rysk koppling*.

⁶¹ Henrik Wachtmeister, "Kinesisk närvaro i den svenska vindkraftssektorn: sårbarheter och risker", *kinesisk-narvaro-i-den-svenska-vindkraftssektorn-sarbarheter-och-risker.pdf*, publicerad 2025.

4.5 Utkontraktering och osäkra leveranskedjor

Det privata näringslivet ansvarar i stor utsträckning för viktiga leveranser till samhällsviktiga verksamheter. Globaliseringen innebär att dessa verksamheters leverantörer ofta finns utanför Sveriges gränser.

Leverantörskedjor möjliggör flera angreppssätt för en angripare. Ju längre leverantörskedja, desto fler potentiella angreppspunkter finns för angriparen. En antagonist kan också, i syfte att komma åt den kritiska verksamheten, bli en leverantör av kritisk utrustning.

Inom elförsörjningen finns ett stort beroende av entreprenörer och leverantörer för både byggnation, underhåll, reparationer och kritiska komponenter, även från utlandet. Det finns vissa leverantörer som tillhandahåller verksamhetskritiska tjänster eller komponenter åt flera nordiska och europeiska systemoperatörer inom elförsörjningen. Vid ett eventuellt angrepp mot dessa leverantörer, eller mot tjänster som dessa leverantörer tillhandahåller, finns en risk för en kaskadeffekt i de verksamheter som anlitar samma leverantör. Antagonisters insteg i leverantörskedjor och delägarskap i företag som är leverantörer och entreprenörer till elsektorn kan inte uteslutas. Detta gäller såväl leverantörer av hård- och mjukvara som konsulttjänster.

Genom att delta i leveranskedjan kan spionutrustning planteras i kritiska komponenter som används inom elförsörjningen. Det går inte att utesluta att en kvalificerad angripare planterar avancerad skadlig kod i hårdvara som sedan köps in och används i samhällskritiska IT-system eller OT-system. Till detta tillkommer även så kallade LOTL-tekniker⁶² där befintlig programvara används som ingång för en attack.

En hotaktör kan också leverera komprometterad hårdvara som gör obehörig åtkomst eller fjärrstyrning möjlig.⁶³

4.5.1 Aktuella händelser

Den cyberkriminella gruppen Clop utnyttjade 2023 en noll dagarssårbarhet i företaget MOVEit:s filöverföringsplattform som används av flera tusen

⁶² Living-off-the-Land (LOTL)

⁶³ Myndigheten för civilt försvar, *Cyberangreppens utveckling 2023-2025 – Årsrapport cyberincidentrapportering 2025*.

myndigheter och företag.⁶⁴ Bland de drabbade återfinns bl.a. Schneider Electric och Siemens Energy som är stora leverantörer av industriella kontrollsystem (ICS). Clop har genom sårbarheten lyckats utpressa hundratals organisationer genom att kompromettera en enda miljö. Omfattningen av attacken påvisade flera brister hos de drabbade, men även komplexiteten kring att säkra hela leverantörskedjan.⁶⁵

I början av 2024 drabbades ett av IT-leverantören TietoEvrys datacenter av en ransomware-attack som fick stor påverkan på svenska företag och myndigheter. Gruppen Akira tros ligga bakom attacken, som utförts genom att utnyttja en sårbarhet i underleverantören Ciscos produkter.⁶⁶ Händelsen visar på många myndigheters och organisationers bristande beredskap för plötsligt bortfall, samt riskerna med att flera verksamheter nyttjar samma leverantörer.⁶⁷

Ett exempel på komprometterad hårdvara är kinesiska växelriktare. Under våren 2025 rapporterades att otillåtna dolda mobilradiomoduler hade upptäckts i kinesiska växelriktare i solcellsparker i USA och Europa. Upptäckten av detta tyder på att angripare skulle kunna fjärraktivera enheterna för att stänga av eller skada dem på distans.⁶⁸

4.6 Informationspåverkan

Myndigheten för psykologiskt försvar (MPF) beskriver otillbörlig informationspåverkan som ett ökande säkerhetshot där främmande makt utnyttjar samhällets sårbarheter genom exempelvis desinformation, vilseledning och propaganda.⁶⁹

⁶⁴ CERT-SE, "Kritisk sårbarhet i MOVEit Transfer", <https://www.cert.se/2023/06/kritisk-sarbarhet-i-moveit-transfer>, publicerad 2023-06-01.

⁶⁵ Emsisoft, "Unpacking the MOVEit Breach: Statistics and Analysis", <https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/>, publicerad 2023-07-23.

⁶⁶ Computer Sweden, "Cyberattack mot Tietoevry slår hårt – många drabbade", <https://computersweden.se/article/1296140/cyberattack-mot-tietoevry-slar-hart-manga-drabbade.html>, publicerad 2024-01-22.

⁶⁷ Regeringskansliet, "Regeringen samlade berörda myndigheter med anledning av storskalig cyberattack", [Regeringen samlade berörda myndigheter med anledning av storskalig cyberattack – Regeringen.se](https://www.regeringen.se/press/2024/01/30/regeringen-samlade-berorda-myndigheter-med-anledning-av-storskalig-cyberattack), publicerad 2024-01-30.

⁶⁸ Myndigheten för civilt försvar, *Cyberangreppens utveckling 2023-2025 – Årsrapport cyberincidentrapportering 2025*.

⁶⁹ Myndigheten för psykologiskt försvar, "Otillbörlig informationspåverkan från främmande makt", *Otillbörlig informationspåverkan från främmande makt | Myndigheten för psykologiskt försvar*, publicerad 2025-03-07.

Otillbörlig informationspåverkan mot elförsörjningen kan syfta till att påverka människors uppfattningar, beslut och beteenden, genom att med desinformation skapa osäkerhet, misstro och polarisering. Det kan exempelvis ske genom att underminera förtroendet för myndigheter, energibolag, elmarknaden och elförsörjningen i stort. Frågor som kan vara föremål för informationspåverkan är sådana som redan är omdebatterade, polariserade eller som personer kan känna oro eller misstro kring. Exempel på detta kan vara att skapa eller förstärka oro kring elbrist, höga elpriser eller störningar i elförsörjningen. Vid händelse av kriser eller incidenter kan spridandet av falska, missvisande eller vinklade narrativ om de bakomliggande orsakerna utgöra informationspåverkan. Informationspåverkan kan också förekomma i form av att förstärka konflikter och polarisering kring ställningstaganden beträffande olika energislag.

I flera sammanhang, bland annat opinionsbildning och reklam, används information i syfte att påverka den eller de målgrupper som informationen riktas mot. Kommunikation i syfte att påverka är således en naturlig del i ett demokratiskt samhälle och ska inte förväxlas med otillbörlig informationspåverkan. MPF lyfter tre väsentliga indikationer som kan användas för att identifiera eventuell otillbörlig informationspåverkan:

- *Vilseledande.* Är kommunikationen medvetet vilseledande, det vill säga förmedlas uppgifter som är falska eller som som vinklas på ett vilseledande sätt? Kan innehållet i kommunikationen verifieras?
- *Avsiktlig.* Bidrar kommunikationen till konstruktiv debatt, även om innehållet är kontroversiellt i sig? Otillbörlig informationspåverkan syftar till motsatsen – den sker med avsikt att försvaga eller sabotera regler, normer och det system som ett demokratiskt samhälle vilar på.
- *Störande.* Tillförlitlig kommunikation är en naturlig del av samhället och stärker demokratin, även sådan som i vissa fall skapar friktion. Otillbörlig informationspåverkan däremot stör och försvagar det demokratiska samtalet och samhällets funktionalitet.⁷⁰

Ryssland har sedan lång tid tillbaka bedrivit informationspåverkan mot Sverige och Europa i stort. Enligt Säkerhetspolisen kommer detta att vara något som den ryska regimen fortsätter att prioritera.

⁷⁰ Ibid.

Informationspåverkan från den ryska regimen syftar till att säkerställa dess fortlevnad, försvaga Nato-samarbetet samt underminera stödet till Ukraina. Narrativ som ofta används i regimen informationspåverkan är sådana där andra stater utmålas som Rysslandsfientliga eller som innehåller budskap som förstärker splittring kring frågor som redan är polariserade i ett samhälle.⁷¹

4.6.1 Aktuella händelser

Ett exempel på informationspåverkan kopplat till europeisk elförsörjning är narrativ från Kreml-kopplade medier om att européer kommer att frysa på vintern utan rysk olja och gas. Liknande narrativ sprids även kring att den Europeiska unionen (EU) utan leverans av ryska fossila bränslen oundvikligen kommer att stagnera och går mot ekonomisk och politisk kollaps.⁷²

MPF uttalade sig under 2022 om att Ryssland sedan 2015 bedrivit en lågintensiv påverkanskampanj mot Sverige inom bland annat energi- och klimatområdet.⁷³ Frågor inom elförsörjningen som är polariserade kan utgöra mål för främmande makts informationspåverkan i syfte att öka befintlig splittring, missnöje eller osäkerhet.

I kölvattnet av det omfattande strömavbrottet på den iberiska halvön och i delar av Frankrike under 2025 spreds såväl missinformation som desinformation. Bland annat spreds påståenden om att den bakomliggande orsaken var en cyberattack och en terroristattack. Ett annat felaktigt påstående som spreds strax efter strömavbrottet var att den Europeiska kommissionens ordförande Ursula von der Leyen hade gått ut och anklagat Ryssland för att, genom en cyberattack, ha orsakat strömavbrottet. Spaniens premiärminister uttalade sig till nationen om att den kris som strömavbrottet utgjorde innebar perfekta omständigheter för missinformation och lögn, samt uppmanade personer att inte sprida information från tveksamma källor.⁷⁴

⁷¹ Säkerhetspolisen (2026), *Lägesbild 2025-2026*.

⁷² East StratCom Task Force, "Only acceptable measure for the EU to avoid an energy crisis is to bring Russian energy back", Disinfo: Only acceptable measure for the EU to avoid an energy crisis is to bring Russian energy back, publicerad 2026-04-03.

⁷³ Aktuell Hållbarhet, "Så bedriver Ryssland desinformation på energi- och klimatområdet – "Lågintensiv påverkanskampanj", Rysk desinformation som bromsar klimatomställningen - så ser den ut enligt Myndigheten för psykologiskt försvar. - Aktuell Hållbarhet, publicerad 2022-07-20.

⁷⁴ Euronews, "Iberian Peninsula blackout sparks spread of false theories online", Iberian Peninsula blackout sparks spread of false theories online | Euronews, publicerad 2025-04-29.

Ett exempel utanför elförsörjningen, som har beskrivits som den största informationspåverkanskampanjen Sverige utsatts för, är den så kallade LVU-kampanjen. I början av 2022 uppmärksammades den otillbörliga informationspåverkanskampanjen som kretsade kring den svenska socialtjänsten och Lagen med särskilda bestämmelser om vård av unga (LVU). Narrativ spreds om att socialtjänsten kidnappar barn och att de särskilt riktar in sig på barn med utländskt påbrå och muslimsk trosuppfattning.

Kampanjen kom att få en internationell dimension och det har påvisats hur aktörer med kopplingar till radikalislamistiska miljöer främjade och bidrog till att sprida dessa narrativ. Till följd av informationspåverkanskampanjen förekom hat och hot mot svenska offentliga institutioner och enskilda socialsekreterare. Det förekom även uppmaningar till våld och terrorattentat. Mer om LVU-kampanjen går bland annat att läsa i den rapport Försvarshögskolan gjort på uppdrag av MPF, *LVU-kampanjen: Desinformation, konspirationsteorier och kopplingarna mellan det inhemska och det internationella i relation till informationspåverkan från icke-statliga aktörer*.⁷⁵

⁷⁵ Försvarshögskolan (2023), *LVU-kampanjen*.

Referenser i urval

Samlingssidor för svenska underrättelsemyndigheters årsöversikter

Säkerhetspolisens lägesbilder - Säkerhetspolisen

Årsrapporter - FRA

Must årsöversikt

Publikationer från NCT - Säkerhetspolisen

Svenska myndigheter i övrigt

Ekobrottsmyndigheten. (2025) *Myndighetsgemensam lägesbild 2025*.

<https://www.ekobrottsmyndigheten.se/wp-content/uploads/se/2025/08/myndighetsgemensam-lagesbild-2025.pdf>

Myndigheten för civilt försvar. (2026) *Cyberangreppens utveckling 2023–2025 : Årsrapport cyberincidentrapportering 2025*,

<https://rib.msb.se/filer/pdf/31323.pdf>

Totalförsvarets forskningsinstitut. (2026). *Publika data som riskfaktor: En förstudie om påverkan på informationssäkerhet och säkerhetsskydd (FOI-R--5931--SE)*. <https://www.foi.se/rest-api/report/FOI-R--5931--SE>

Totalförsvarets forskningsinstitut. (2026). *“Spies Among Us”: Espionage in Europe – A study on convicted spies in Europe 2008–2024 (FOI-R--5866--SE)*.

<https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5866--S>

Myndigheten för psykologiskt försvar. (u.å.). *Otillbörlig informationspåverkan från främmande makt*. <https://mpf.se/kunskap-och-stod/formageportalen/forebygga/otillborlig-informationspaverkan-fran-frammande-makt>

Nationellt cybersäkerhetscenter. (2025). *Överbelastningsangrepp mot kritisk infrastruktur i Norden och Baltikum hösten 2024: Tillvägagångssätt, infrastruktur och rekommendationer*.

https://www.ncsc.se/siteassets/publikationer/overbelastningsangrepp_mot_kritisk_infrastruktur_norden_baltikum_2024.pdf

Utländska myndigheter

CERT-EU. (2026). *Threat Landscape Report 2025: A year in review*.
<https://www.cert.europa.eu/publications/threat-intelligence/tlr2025/pdf>

European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Threat Landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

CERT Polska. (2026). *Energy Sector Incident Report – 29 December 2025*.
https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf